Соблюдение «компьютерной гигиены» - залог защиты от мошенничества в сфере цифровых технологий

В последние годы в нашу жизнь стремительно ворвался интернет. Он охватывает практически все стороны нашей деятельности. Большинство граждан нашей страны, все больше времени проводят в интернете и с каждым днем возрастает количество совершаемых ими покупок различных товаров и услуг в режиме онлайн.

Это, конечно, очень удобно, но таит в себе большую опасность, так как злоумышленники с развитием новых технологий придумывают все новые схемы мошенничества, а значит, без определенных, базовых знаний в области кибербезопасности нам не обойтись.

Как известно, в цифровом пространстве есть свои определенные правила гигиены. Компьютерная гигиена так же необходима, как и медицинская гигиена. Она предназначена для профилактики заражения компьютера или смартфона вирусами и разного рода вредоносными программными обеспечениями.

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Ингушетия

В большинстве случаев, согласно исследованиям, мы сами виноваты в том, что наши компьютеры и смартфоны заражены вредоносными программами, чем даем мошенникам возможность в совершении в отношении нас противоправных действий.

Иными словами, подавляющее большинство атак в интернете мошенники совершают используя человеческий фактор, а не уязвимость операционной системы.

К использованию интернета необходимо относится очень серьезно, нужно понимать, что необдуманные действия в сети интернет могут привести к печальным последствиям.

Напомним о некоторых правилах информационной безопасности, которых необходимо придерживаться во избежание противоправных действий со стороны мошенников:

- Старайтесь не рассказывать о себе в интернете. Прежде чем что-либо сообщить, подумайте, кому и что вы хотите сообщить. Ведь мошенники могут воспользоваться, и зачастую пользуются информацией, полученной от вас самих.

- Ни в коем случае не передавайте свой телефон незнакомым людям, к примеру, встретившимся вам на улице, у которых якобы разрядился телефон, а им нужно срочно позвонить.

- Необходимо пользоваться надежными паролями, особенно для операций, связанных с платежами и денежными переводами. Помните, что чем длиннее пароль, тем он сложнее, что намного усложнит злоумышленникам доступ к вашей информации и затруднит совершение противоправных действий.

- Почаще обновляйте программы и операционные системы ваших компьютеров и смартфонов. Разработчики программ постоянно работают над повышением уровня их защиты.

- Не открывайте электронные письма, поступившие от неизвестных вам адресатов. Они могут быть заражены и соответственно, могут доставить вам массу проблем.

- При обращении к своему мобильному банку не пользуйтесь публичными сетями Wi-Fi. Вероятность внедрения мошенников в публичные сети очень велика.

- Никому не сообщайте данные своей банковской карты, в том числе банковским служащим и работникам интернет-магазинов.

- не используйте подозрительные Интернет-сайты.

- подключите к своему устройству СМС-оповещение.

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Ингушетия

- Не открывайте письма, поступившие в спам.

- Не знакомьтесь с незнакомыми людьми в социальных сетях и не принимайте их запросы на дружбу.

-Всегда используйте антивирус и регулярно проверяйте свое устройство на наличие вирусов.

- будьте осмотрительными и проверяйте доступным способом информацию, прежде чем перечислять денежные средства при приобретении товара через интернет-магазин.

Перечисленные, простые правила помогут вам не попасть в сложную, неприятную ситуацию и избежать противоправных действий со стороны мошенников.

Напомним, что за мошенничество с использованием электронных средств платежа предусмотрена уголовная ответственность в соответствии со статьей 159.3 Уголовного кодекса Российской Федерации. Согласно Федеральному закону от 27.06.2011 № 161-ФЗ «О национальной платежной системе», электронное средство платежа - средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

В соответствии со статьей 159.6 Уголовного кодекса Российской Федерации предусмотрена уголовная ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

В зависимости от тяжести совершенного преступления Уголовным кодексом Российской Федерации за преступления, связанные с указанными видами мошеннических действий, предусмотрено наказание в виде штрафа, обязательных, исправительных и принудительных работ, либо лишением свободы на срок до десяти лет.

27 Мая 2021

Адрес страницы: https://ingushetia.sledcom.ru/news/item/1573999

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Ингушетия

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Ингушетия